Cuestionario Auditoría TI

Fecha: 17 de junio de 2018

Autores

Paula González Mataix - paulagonzalezmataix@gmail.com

José Vicente Berná Martínez – jvberna@ua.es

Versión: 1.1

Título: Cuestionario para auditoría TI

Palabras clave: auditoría TI, cuestionario, planificación, almacenamiento, centro de cómputo, seguridad física

Descripción

En este documento se recoge el cuestionario usado en el Trabajo de Fin de Grado del Grado de Ingeniería Informática de la Universidad de Alicante, de la alumna Paula González Mataix y dirigido por el Dr. José Vicente Berná Martínez, titulado ***Auditoría TI en la asociación APSA***, presentado en septiembre de 2018.

El objetivo de ese cuestionario es el de recolectar la información suficiente sobre ciertos aspectos TI de una empresa para emitir un informe auditor que permite alinear la TI de la empresa con sus necesidades actuales y futuras, en las áreas objeto del estudio.

El cuestionario está dividido en cuatro bloques temáticos, uno por cada área que ha sido objeto de estudio. El primer bloque es el correspondiente al área de planificación y tiene como objetivo sondear la planeación que se realizó para formar el área de sistemas. El segundo bloque es el correspondiente a los dispositivos de almacenamiento y tiene como objetivo evaluar la administración, la aplicación y el uso de dispositivos hardware de almacenamiento de información electrónico de la organización. El tercer bloque es el correspondiente al funcionamiento del centro de cómputo y tiene como objetivo evaluar el correcto funcionamiento y la organización del centro de cómputo. El cuarto bloque es el correspondiente a la seguridad física y su objetivo es verificar la seguridad física de las instalaciones que utiliza el área de sistemas.

Bloque I - Planificación

El primer bloque de preguntas del cuestionario de auditoría que vamos a realizar es el correspondiente al área de planificación que se divide en las preguntas correspondientes a sistemas de información, a recursos humanos y a otros aspectos correspondientes al área de planificación, teniendo como objetivo sondear la planeación que se realizó para formar el área de sistemas, siendo de vital importancia para el desempeño del área, pues verifica si los objetivos y los alcances del área corresponden a los desempeñados.

Cuestionario de Auditoría correspondiente al área de planificación:

1. Sistemas de información

1.1 ¿La dirección general y ejecutiva ha considerado la importancia que tiene el estudio del sistema de información?

SI ( ) NO ( )

1.2 ¿Se establecen los requisitos de información a largo plazo?

SI ( ) NO ( )

1.3 ¿Se ha realizado una planificación estratégica del sistema de información para la Empresa?

SI ( ) NO ( )

1.4 ¿Existe una metodología para llevar a cabo tal planificación?

SI ( ) NO ( )

1.5 ¿Está definida la función del director del sistema de información?

SI ( ) NO ( )

1.6 ¿Existe un plan estratégico del departamento de sistema de información?

SI ( ) NO ( )

2. Recursos humanos

2.1 ¿Se estudia la evolución del mercado y la adaptación del personal a esa evolución?

SI ( ) NO ( )

2.2 ¿Los informáticos reciben noticias del momento tecnológico por revistas, notas técnicas, etc.?

SI ( ) NO ( )

2.3 ¿Se recibe formación y se planifica ésta mediante asistencia a cursos, seminarios, etc.?

SI ( ) NO ( )

3. Otros aspectos

3.1 ¿Los cambios en los sistemas informáticos son consecuencia de la planificación más que de la presión por necesidades operativas?

SI ( ) NO ( )

3.2 ¿Se solicitan demostraciones sobre los nuevos artículos a los proveedores?

SI ( ) NO ( )

3.3 ¿Se ha realizado algún estudio de planificación del posible efecto de las cargas normales de trabajo y los picos sobre los requerimientos tanto de equipos como de software?

SI ( ) NO ( )

3.4 ¿La entidad dispone de un plan informático?

SI ( ) NO ( )

3.5 ¿Se están siguiendo las directrices marcadas por el plan?

SI ( ) NO ( )

3.6 ¿El plan recoge todos los diferentes aspectos relacionados con la función informática?

SI ( ) NO ( )

3.7 ¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?

Bloque II - Almacenamiento

El segundo cuestionario es el correspondiente a los dispositivos de almacenamiento y este cuestionario tiene como objetivo evaluar la administración, la aplicación y el uso de dispositivos, hardware, de almacenamiento de información electrónico de la organización.

Cuestionario de Auditoría correspondiente a los dispositivos de almacenamiento:

1. Los locales asignados a los servidores de datos tienen

   • Aire acondicionado ( )

   • Protección contra el fuego ( )

   • Cerradura especial ( )

   • Otra:

2. ¿Tienen los servidores de datos protección automática contra el fuego?

   SI ( ) NO ( )

   (Señalar de que tipo)

3. ¿Qué información mínima contiene el inventario de los servidores de datos?

Número de serie o carrete ( )

Número o clave del usuario ( )

Número del archivo lógico ( )

Nombre del sistema que lo genera ( )

Fecha de expiración del archivo ( )

Número de volumen ( )

Otros

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?

SI ( ) NO ( )

5. ¿En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias?

SI ( ) NO ( )

6. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido?

SI ( ) NO ( )

7. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?

SI ( ) NO ( )

¿Cómo se tienen identificados los archivos con información confidencial?

¿Con que tipo de claves de acceso se cuenta?

8. ¿Existe un control estricto de las copias de estos archivos?

SI ( ) NO ( )

9. ¿Qué medio se utiliza para almacenarlos?

Mueble con cerradura ( )

Bóveda ( )

Otro (especifique):

10. Este almacén está situado:

En el mismo edificio del departamento ( )

En otro lugar ( ) ¿Cuál?:

11. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?

SI ( ) NO ( )

12. ¿Se certifica la destrucción o baja de los archivos defectuosos?

SI ( ) NO ( )

13. ¿Se registran como parte del inventario las nuevas cintas que recibe la biblioteca?

SI ( ) NO ( )

14. ¿Se tiene un responsable, por turno, de los servidores de datos?

SI ( ) NO ( )

15. ¿Se realizan auditorías periódicas a los medios de almacenamiento?

SI ( ) NO ( )

16. ¿Qué medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

17. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?

SI ( ) NO ( )

18. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?

SI ( ) NO ( )

19. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?

SI ( ) NO ( )

20. ¿Se lleva control sobre los archivos prestados por la instalación?

SI ( ) NO ( )

21. En caso de préstamo ¿Con que información se documentan?

Nombre de la institución a quién se hace el préstamo.

Fecha de recepción ( )

Fecha en que se debe devolver ( )

Archivos que contiene

Formatos

Cifras de control ( )

Código de grabación ( )

Nombre del responsable que los presto

Otros

22. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros:

23. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?

SI ( ) NO ( )

24. ¿La operación de reemplazo es controlada por el operador?

SI ( ) NO ( )

25. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?

SI ( ) NO ( )

26. ¿Estos procedimientos para recuperar los archivos los conocen los operadores?

SI ( ) NO ( )

27. ¿Con que periodicidad se revisan estos procedimientos?

MENSUAL ( ) ANUAL ( )

SEMESTRAL ( ) OTRA ( ):

28. ¿Existe un responsable en caso de falla?

SI ( ) NO ( )

29. ¿Existe un procedimiento para el manejo de la información del *cuarto frío*?

SI ( ) NO ( )

30. ¿El procedimiento para el manejo de la información del cuarto frío lo conoce y lo sigue el operador?

SI ( ) NO ( )

31. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?

SI ( ) NO ( ) ¿Con qué frecuencia?:

Bloque III – Centro de cómputo

El tercer cuestionario es el correspondiente al funcionamiento del centro de cómputo y este cuestionario tiene como objetivo evaluar el correcto funcionamiento, así como la organización del centro de cómputo, tomando en cuenta los reglamentos del área. Así como también revisar que estos reglamentos tengan como objetivo mantener el orden del centro de cómputo.

Cuestionario de Auditoría correspondiente al funcionamiento del centro de cómputo:

1. ¿El lugar donde se ubica el centro de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos?

   SI ( ) NO ( )

2. ¿El centro de cómputo da hacia el exterior?

   SI ( ) NO ( )

3. ¿El material con que está construido el centro de cómputo es confiable?

   SI ( ) NO ( )

4. ¿Dentro del centro de cómputo existen materiales que puedan ser inflamables o causar algún daño a los equipos?

   SI ( ) NO ( ) ¿Cuál?:

5. ¿Existe lugar suficiente para los equipos?

   SI ( ) NO ( )

6. ¿Aparte del centro de cómputo se cuenta con algún lugar para almacenar otros equipos de cómputo, muebles, suministros, etc.?

SI ( ) NO ( ) ¿Dónde?:

7. ¿Se cuenta con una salida de emergencia?

SI ( ) NO ( )

8. ¿Existen señalamientos que hagan visibles las salidas de emergencia?

SI ( ) NO ( ) ¿Dónde?:

9. ¿Es suficiente la iluminación del centro de cómputo?

SI ( ) NO ( ) ¿Por qué?:

10. ¿La temperatura a la que trabajan los equipos es la adecuada de acuerdo a las normas bajo las cuales se rige?

SI ( ) NO ( )

11. ¿Se dispone de aire acondicionado?

SI ( ) NO ( )

12. ¿La ubicación de los aires acondicionado es adecuada?

SI ( ) NO ( )

13. ¿Existe algún otro medio de ventilación aparte del aire acondicionado?

SI ( ) NO ( ) ¿Cuál?:

14. ¿El aire acondicionado emite algún tipo de ruido?

SI ( ) NO ( )

15. ¿El cableado se encuentra correctamente instalado?

SI ( ) NO ( )

16. ¿Se cuenta con los planos de instalación eléctrica?

SI ( ) NO ( )

17. ¿La instalación eléctrica del equipo de cómputo es independiente de otras instalaciones?

SI ( ) NO ( )

18. ¿Los equipos cuentan con un regulador?

SI ( ) NO ( )

19. ¿Se cuenta con equipo interrumpible?

SI ( ) NO ( )

20. ¿Se tiene switch de apagado en caso de emergencia en algún lugar visible?

SI ( ) NO ( )

21. ¿Los cables están dentro de paneles y canales eléctricos?

SI ( ) NO ( )

22. ¿Los interruptores de energía están debidamente protegidos y sin obstáculos para alcanzarlos?

SI ( ) NO ( )

23. ¿Se cuenta con alarma contra incendios?

SI ( ) NO ( )

24. ¿Dónde se encuentran ubicadas las alarmas contra incendios?

25. ¿Se cuenta con alarmas contra inundaciones?

SI ( ) NO ( )

26. ¿Dónde se encuentran ubicadas las alarmas contra inundaciones?

27. ¿Existen extintores?

SI ( ) ¿Cuántos?:_____ NO ( )

Tipos de extintores: Manual ( ) Automático ( ) No existen ( )

28. ¿Hay algún tipo de control de entradas y salidas de usuario?

SI ( ) NO ( )

29. ¿El usuario respeta el control de entradas y salidas de usuario?

SI ( ) NO ( )

30. ¿Con que tipo de programas cuentan en los equipos de cómputo?

31. ¿Cuentan con manuales para cada programa que se maneja?

SI ( ) NO ( )

32. ¿El personal sabe del contenido de estos manuales para cada programa?

SI ( ) NO ( )

33. ¿Qué tipo de mantenimiento realizan de los programas?

A. Preventivo ( ) B. Correctivo ( )

34. ¿Por qué razón realizan ese tipo de mantenimiento?

35. ¿Qué materiales utilizan para realizar el mantenimiento del hardware?

36. ¿Tienen un lugar específico para guardar el material de mantenimiento de hardware?

SI ( ) NO ( )

37. ¿Qué materiales utilizan para realizar el mantenimiento de software?

38. ¿Tienen un lugar específico para guardar el material de mantenimiento de software?

SI ( ) NO ( )

39. ¿Los usuarios tienen la suficiente confianza como para presentar su queja si fallasen los equipos?

SI ( ) NO ( )

40. ¿Se efectúan controles o revisiones del buen estado de los equipos de cómputo?

SI ( ) NO ( )

41. ¿Las inspecciones son realizadas por personal especializado como técnicos o mecánicos electrónicos?

SI ( ) NO ( )

42. ¿Los datos de clientes y proveedores se salvaguardan por parte del sistema?

SI ( ) NO ( )

43. ¿Se implementan medidas de seguridad en los computadores de los empleados para evitar que estos ejecuten programas peligrosos?

SI ( ) NO ( )

44. ¿Existe un programa de protección de la información contra virus, spyware y diferentes ataques cibernéticos?

SI ( ) NO ( )

45. ¿Se usan claves para acceder a las bases de datos?

SI ( ) NO ( )

46. ¿Todos los empleados pueden acceder a estas?

SI ( ) NO ( )

Bloque IV – Seguridad física

El cuarto cuestionario es el correspondiente a la seguridad física y este cuestionario verifica la seguridad física de las instalaciones que utiliza el área de sistemas, ya que de esto depende la continuidad de los servicios que presta el área a la organización, en cuanto a necesidades de información.

Cuestionario de Auditoría correspondiente a la seguridad física:

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?

   SI ( ) NO ( )

2. ¿Existen una persona responsable de la seguridad?

   SI ( ) NO ( )

3. ¿Existe personal de vigilancia en la institución?

   SI ( ) NO ( )

4. ¿La vigilancia se contrata?

   Directamente ( )
   Por medio de empresas que venden ese servicio ( )

5. ¿Existe una clara definición de funciones entre los puestos clave?

   SI ( ) NO ( )

6. ¿Se investiga a los vigilantes cuando son contratados directamente?

   SI ( ) NO ( )

7. ¿Se controla el trabajo fuera de horario?

   SI ( ) NO ( )

8. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?

SI ( ) NO ( )

9. ¿Existe vigilancia en el departamento de cómputo las 24 horas?

SI ( ) NO ( )

10. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?

Vigilante ( )
Recepcionista ( )
Tarjeta de control de acceso ( )
Nadie ( )

11. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?

SI ( ) NO ( )

12. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?

SI ( ) NO ( )

13. El edificio donde se encuentra la computadora está situado a salvo de:

Inundación ( )
Terremoto ( )
Fuego ( )
Sabotaje ( )
Nada ( )

14. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que construirlo y equipo (muebles, sillas, etc.) dentro del centro.

15. ¿Existe control en el acceso a este cuarto?

Por identificación personal ( )

Por tarjeta magnética ( )

Por claves verbales ( )

Otras ( )

16. ¿Son controladas las visitas y demostraciones en el centro de cómputo?

SI ( ) NO ( )

17. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?

SI ( ) NO ( )

18. Existe alarma en las instalaciones para:

Detectar fuego (calor o humo) de forma automática ( )

Avisar en forma manual la presencia del fuego ( )

Detectar una fuga de agua ( )

Detectar magnéticos ( )

No existe ( )

20. Estas alarmas están:

En el departamento de cómputo ( )

En el cuarto frío ( )

No están ( )

Otros:

21. ¿Existe alarma para detectar condiciones anormales del ambiente?

En el departamento de cómputo ( )

En el cuarto frío ( )

En otros lados:

22. ¿La alarma es perfectamente audible?

SI ( ) NO ( )

23. Esta alarma también está conectada:

Al puesto de guardias ( )

A la estación de bomberos ( )

A ningún otro lado ( )

Otros:

24. Existen extintores de fuego

Manuales ( )

Automáticos ( )

No existen ( )

25. ¿Se ha adiestrado el personal en el manejo de los extintores?

SI ( ) NO ( )

26. Los extintores, manuales o automáticos a base de

Agua ( )

Gas ( )

Otros ( )

27. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?

SI ( ) NO ( )

28. ¿Si es que existen extintores automáticos son activados por detectores automáticos de fuego?

SI ( ) NO ( )

29. Si los extintores automáticos son a base de agua, ¿se han tomado medidas para evitar que el agua cause más daño que el fuego?

SI ( ) NO ( )

30. ¿Si los extintores automáticos son a base de gas?, ¿se ha tomado medidas para evitar que el gas cause más daño que el fuego?

SI ( ) NO ( )

31. Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal:

¿Corte la acción de los extintores por tratarse de falsas alarmas? SI ( ) NO ( )
¿Pueda cortar la energía eléctrica? SI ( ) NO ( )
¿Pueda abandonar el local sin peligro de intoxicación? SI ( ) NO ( )
¿Es inmediata su acción? SI ( ) NO ( )

32. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

SI ( ) NO ( )

33. ¿Existe salida de emergencia? SI ( ) NO ( )

34. Esta puerta solo es posible abrirla:

¿Desde el interior? ( )
¿Desde el exterior? ( )
Ambos lados ( )

35. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?

SI ( ) NO ( )

36. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?

SI ( ) NO ( )

37. Se ha tomado medidas para minimizar la posibilidad de fuego:

Evitando artículos inflamables en el departamento de cómputo ( )
Prohibiendo fumar a los operadores en el interior ( )
Vigilando y manteniendo el sistema eléctrico ( )
No se ha previsto ( )

38. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?

SI ( ) NO ( )

39. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?

SI ( ) NO ( )

40. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?

Usuario ( )
Director de informática ( )
Jefe de análisis y programación ( )
Programador ( )
Otras (especifique):

41. Las solicitudes de modificaciones a los programas se hacen en forma:

Oral ( )
Escrita ( )

42. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?

SI ( ) NO ( )

43. ¿Existe control estricto en las modificaciones?

SI ( ) NO ( )

44. ¿Si se tienen terminales conectadas?, ¿se ha establecido procedimientos de operación?

SI ( ) NO ( )

45. Se verifica identificación:

De la terminal ( )
Del usuario ( )
No se pide identificación ( )

46. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esta terminal y se de aviso al responsable de ella?

SI ( ) NO ( )

49. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones? ¿Cuáles son?

( ) Recepción de documentos

( ) Información confidencial

( ) Captación de documentos

( ) Cómputo electrónico

( ) Programas

( ) Documentos de salida

( ) Archivos magnéticos

( ) Operación del equipo de computación

( ) En cuanto al acceso de personal

( ) Identificación del personal

( ) Policía

( ) Seguros contra robo e incendio

( ) Cajas de seguridad

( ) Otras (especifique)
